

NOTICE

U.S. DEPARTMENT OF TRANSPORTATION FEDERAL AVIATION ADMINISTRATION

N JO 6480.24

Air Traffic Organization Policy

Effective Date:
January 15, 2013

Cancellation Date:
January 15, 2014

NOTICE OF INTENT

SUBJ: Release JO 6480.24, Maintenance of the TBFM System

1. Purpose. This notice advises all Time Based Flow Management (TBFM) stakeholders of the intent to publish a new handbook, JO 6480.24, Maintenance of the Time Based Flow Management System. Information is being solicited for use in preparation of this release.

2. Audience. This notice requires actions by Field Offices at operational facilities with Facility, Service, and Equipment Profile (FSEP) equipment: TBFM.

3. Where Can I Find This Notice? An electronic version of this notice can be obtained from the following websites:

- MYFAA website at https://employees.faa.gov/tools_resources/orders_notices/;
- National Airspace System (NAS) Documentation Electronic Library website at <http://skil.act.faa.gov/AJW-172/library/default.aspx>.
- En Route & Oceanic Support website at <https://enroutesupport.faa.gov>.

4. Action.

a. The recipients of this notice who are concerned with the equipment operation, maintenance, or training of TBFM are requested to furnish, from their own activities or other sources, their recommendations to be used in the release of the subject handbook. Actual field experience factors should be cited when recommending changes to existing standards, tolerances, key inspection elements, daily performance check requirements, and maintenance schedules and procedures. Recommendations should be stated in specific terms. However, it is unnecessary to submit recommendations in the exact handbook format as this will be accomplished during the revision process. A draft of the handbook is attached as Attachment 1, Draft JO 6480.24, Maintenance of the Time Based Flow Management System.

b. Technical Operations offices should arrange to obtain handbook recommendations and submit them to Technical Operations by March 15, 2013.

c. Other offices not included in paragraph 4b should collect, consolidate, and provide input to TBFM Second Level Engineering (SLE) by March 15, 2013.

d. Our goal is to distribute the revised handbook during the second quarter of fiscal year (FY) 2013. Recommendations submitted to TBFM SLE later than April 19, 2013 may be held for future revisions.

5. Background. TBFM is a continuation and support of Traffic Management Advisor (TMA), which is at the end of its lifecycle. The TBFM system re-architecture enhancement upgrades the system architecture to reduce cost of ownership; reduce the logistical footprint; maintain compatibility of hardware and software; comply with system performance requirements; simplify monitor and control; add capability; and increase the flexibility of workstations.

6. Clarification or Comments. For further information or comments, please contact the TBFM SLE team via the En Route & Oceanic Support Help Desk at 1-800-337-0308.



for Vincent Capezzuto, Director
Air Traffic Systems AJM-2

01/15/2013

N JO 6480.24

ATTACHMENT 1. DRAFT JO 6480.24, MAINTENANCE OF THE TIME BASED FLOW
MANAGEMENT SYSTEM



**U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION**

AIR TRAFFIC ORGANIZATION POLICY

**ORDER
NUMBER
JO 6480.24**

Effective Date:
Signature date
Implementation Date:

SUBJ: Maintenance of Time Based Flow Management System

This order prescribes technical standards, tolerances, maintenance, and certification requirements for the Time Based Flow Management (TBFM) system. This order provides the necessary guidance, to be used in conjunction with information available in instruction books, for the proper maintenance of the National Airspace System (NAS).

Vincent Capezzuto, Director
Air Traffic Systems, AJM-2

DRAFT

TABLE OF CONTENTS

<i>Paragraph</i>	<i>Page</i>
Chapter 1. General Information and Requirements	1-1
1-1. Purpose of This Order.	1-1
1-2. Audience.....	1-1
1-3. Where Can I Find This Order.	1-1
1-4. Cancellation.	1-1
1-5. Explanation of Policy Changes.	1-1
1-6. Certification.....	1-1
1-7. Aircraft Accident.....	1-1
1-8. Maintenance Procedure.....	1-1
1-9. Risks.....	1-1
1-10. Implementation Date.....	1-2
1-11. Safety.....	1-2
1-12. Facility Shutdowns.....	1-2
1-13. Coordination.....	1-3
1-14. Reliability Centered Maintenance.....	1-3
1-15.- 1-99. Reserved.....	1-3
Chapter 2. Technical Characteristics.....	2-1
2-1. Purpose.....	2-1
2-2. Description.....	2-1
2-3. Theory.....	2-3
2-4. Air Traffic Situations TBFM Addresses.....	2-4
2-5. TBFM Software Processes.....	2-5
2-6. Monitor and Control (M&C).....	2-7
2-7. TBFM Error Handling and Recovery.....	2-9
2-8. Red Hat Enterprise Linux (Release 6) Platform.....	2-9
2-9. Hours of Operation.....	2-10
2-10. TBFM Equipment Configuration.....	2-10
2-11. TBFM Workstations.....	2-11
2-12. Dell Precision T1600n Processor.....	2-13
2-13. IBM x3550 M3 Server.....	2-14
2-14. Dell UltraSharp 2007FP Display.....	2-15
2-15. Dell U3011 Display.....	2-15
2-16. NEC 20" Flat Panel Display (FPD).....	2-16
2-17. RackMount RKP117-S801E Keyboard with KVM.....	2-17
2-18. Printers.....	2-18
2-19. Dell 3130cn Color Printer.....	2-18
2-20. HP Officejet Pro 8000 Enterprise Printer.....	2-19
2-21. Network Hardware.....	2-19
2-22. Cisco 2911/K9 Router.....	2-19
2-23. Cisco 3925/K9 Router.....	2-20

2-24.	Cisco WS-C2960S-24TS-Switch.	2-21
2-25.	Spectrum Controls AC SMARTStart® Switched Power Distribution Unit.	2-21
2-26.	TBFM Hardware Fault Isolation.	2-22
2-27.	- 2-99. Reserved.	2-22
Chapter 3.	TBFM Standards and Tolerances	3-1
3-1.	General.	3-1
	STANDARDS AND TOLERANCES	3-2
Chapter 4.	Maintenance Requirements	4-1
4-1.	General.	4-1
4-2.	FAA Form 6000 Series.....	4-1
Chapter 5.	Maintenance Procedures	5-1
5-1.	General.	5-1
	Section 1. Performance Check Procedures	5-2
5-2.	Reboot Operational and Support Workstations.....	5-2
5-3.- 5.25.	Reserved.....	5-2
	Section 2. Other Maintenance Task Procedures	5-3
5-26.	Clean Air Intake and Exhaust Vents.	5-3
5-27.	Clean Dirty Cabinets.	5-3
5-28.	Adjust FPD Monitor Controls.	5-3
5-29.	Clean FPD Monitor.	5-4
5-30.	Clean Printers.	5-4
	Section 3. Special Maintenance Task Procedures.....	5-6
5-31.	General.	5-6
5-32.- 5.99.	Reserved.....	5-6
Chapter 6.	Flight Inspection.....	6-1
6-1.- 6.99.	Reserved.....	6-1
Appendix 1.	List of Acronyms and Abbreviations.....	A1-1
Appendix 2.	Policy/Procedures for Identifying, Handling, Marking and Disposal of Sensitive Unclassified Information (SUI)	A2-1
A2-1.	Purpose.	A2-1
A2-2.	Scope.	A2-1
A2-3.	Background.	A2-1
A2-4.	Policy.....	A2-1
A2-5.	Types of SUI.	A2-1
A2-6.	Identifying and Working With SUI.....	A2-2
A2-7.	Marking/Labeling SUI.	A2-3
A2-8.	Storing SUI.....	A2-4
A2-9.	Distribution Procedures for SUI.....	A2-4
A2-10.	Disposal of SUI.	A2-6
Appendix 3.	Sensitive Security Information and Magnetic Media Disposal/Reutilization Policy/Procedures.....	A3-1
A3-1.	Purpose.	A3-1

A3-2.	Scope.	A3-1
A3-3.	Background.	A3-1
A3-4.	Policy.	A3-1
A3-5.	Procedures for Sanitizing SBU Electronic Storage Media.	A3-2
A3-6.	Definitions.	A3-4
A3-7.	Acceptable Commercial Software Products.	A3-4
Appendix 4. Administrative Information		A4-1
A4-1.	Distribution.	A4-1
A4-2.	Authority to Change this Order.	A4-1
A4-3.	Related Publications.	A4-1
A4-4.	Forms and Reports.	A4-2
A4-5.	Recommendations for Changes.	A4-2
Appendix 5. Safety Risk Management Decision Memorandum.....		A5-1

DRAFT

LIST OF ILLUSTRATIONS

<i>Figure</i>		<i>Page</i>
Figure 2–1.	TBFM Wide Area Communications Network.....	2–3
Figure 2–2.	TBFM Configuration	2–11
Figure 2–3.	Dell Precision™ T1600n Processor.....	2–14
Figure 2–4.	IBM x3550 M3 Server	2–14
Figure 2–5.	Dell UltraSharp 2007FP Display	2–15
Figure 2–6.	Dell U3011 Display	2–16
Figure 2–7.	NEC LCD 2080UX+BK	2–16
Figure 2–8.	NEC LCD 2090UXI-BK.....	2–17
Figure 2–9.	Rack Mount Monitor, Keyboard, and Switch: RKP117-S801e.....	2–18
Figure 2–10.	Dell 3130cn Color Printer	2–18
Figure 2–11.	Officejet Pro 8000 Enterprise Printer	2–19
Figure 2–12.	Cisco 2911 /K9 Router.....	2–20
Figure 2–13.	Cisco 3925 Router.....	2–20
Figure 2–14.	Cisco WS-C2960S-24TS-S Switch.....	2–21
Figure 2–15.	Spectrum Controls AC SMARTStart® Switched Power Distribution Unit ..	2–22

LIST OF TABLES

<i>Table</i>	<i>Page</i>
Table 2–1. TBFM Workstation Processes	2–13

DRAFT

DRAFT

Chapter 1. General Information and Requirements

1-1. Purpose of This Order. This Maintenance Technical Handbook (MTHB) provides guidance and prescribes technical standards, tolerances, and procedures applicable to the maintenance and inspection of the Time Based Flow Management (TBFM) system. It also provides information on special methods and techniques, which will enable maintenance personnel to achieve optimum performance from the equipment. This information augments information available in Technical Instruction Books (TIB) and other MTHBs, and complements the latest edition of Order 6000.15, General Maintenance Handbook for National Airspace System (NAS) Facilities.

1-2. Audience. This MTHB requires actions by the Field Offices with Facility, Service, and Equipment Profile (FSEP) equipment: TBFM.

1-3. Where Can I Find This Order. . This order may be found on the MyFAA website at: https://employees.faa.gov/tools_resources/orders_notices/.

1-4. Cancellation. . Not applicable.

1-5. Explanation of Policy Changes. This MTHB implements Configuration Control Decision (CCD) TBD.

1-6. Certification. Not applicable.

1-7. Aircraft Accident. When aircraft accidents or incidents occur, Air Traffic Organization (ATO)/Technical Operations personnel are responsible, when requested by the Technical Operations Aircraft Accident Representative (TOAAR) through the appropriate control center, to evaluate and document the technical performance of the facilities which may have been involved (for some facilities, it may also be necessary to remove them from service, and to conduct flight inspections). This requires that facility operational data be obtained and recorded in the maintenance log and on technical performance records. These records are official documents, and may be used by an aircraft accident investigation board in the determination of facility operational status at the time of the accident.

Refer to the latest edition of Order 8020.16, Air Traffic Organization Aircraft Accident and Incident Notification, Investigation, and Reporting, for detailed guidance on requirements and activities following an aircraft accident/incident.

1-8. Maintenance Procedure. Order 6000.15, this MTHB, the applicable equipment TIB, and other applicable handbooks are consulted and used together by the maintenance technician in all duties and activities for the maintenance of TBFM. These documents are considered collectively as the single official source of maintenance policy and direction authorized by Technical Operations Services. References located in the appropriate paragraphs of this handbook entitled Chapter 3, Standards and Tolerances, Chapter 4, Maintenance Requirements, and Chapter 5, Maintenance Procedures, indicate to the user whether this handbook and/or the equipment TIB must be consulted for a particular standard, key inspection element or performance parameter, performance check, maintenance task, or maintenance procedure.

1-9. Risks.

a. Operational. In compliance with the latest edition of Order JO 6000.50, National Airspace System (NAS) Integrated Risk Management, activities are to be assessed for potential risk to the NAS from an operational perspective. The following operational risks are associated with this MTHB:

b. Safety. In compliance with the latest edition of Order 1100.161, Air Traffic Safety Oversight, and JO 1000.37, Air Traffic Organization Safety Management System, all NAS changes require a Safety Risk Management (SRM) assessment for all SSMs prior to delivery. The SRM information for this SSM is available as Appendix 5, Safety Risk Management Decision Memorandum. For further guidance in SRM documentation, refer to the latest edition of the Safety Management System (SMS) Manual. The following safety risks are associated with this MTHB.

c. Security. In compliance with the latest edition of Order 1370.82, Information Systems Security Program, the Federal Aviation Administration (FAA) must ensure that security controls are implemented and commensurate with the risk and magnitude of the harm that would result from the loss, misuse, denial of service, unauthorized access, or modification of Federal information assets. The following security risks are associated with this MTHB:

1-10. Implementation Date. This MTHB must be implemented by *****

1-11. Safety. Maintenance personnel must observe all pertinent safety precautions when performing duties on the equipment covered in this manual. For guidance, refer to the latest edition of Order 6000.15.

1-12. Facility Shutdowns.

a. TBFM site shutdowns are not necessary for maintenance or repair of system components. Site shutdowns will occur when utility power is unavailable for a period long enough to exhaust the capacity of the backup power supplies. For a site shutdown to occur otherwise, any of the following would have to happen:

(1) At sites with two TBFM routers, both would have to fail at the same time. At sites with one router, the single router would have to fail.

(2) A short circuit or nearby lightning strike would have to damage the Ethernet cables to the point where they cannot function.

(3) An occurrence of fire, flood, or other natural disaster that results in damage to equipment or cabling.

b. As long as at least one router and one workstation are functioning, a Local Area Network (LAN) exists and can operate.

c. For the TBFM site to be considered operational (with limited capabilities), the operational router, one Air Route Traffic Control Center (ARTCC) data feed connection, one Monitor and Control (M&C) workstation, one Communications Manager (CM) workstation, one Route Analyzer/Trajectory Synthesizer (RATS) workstation, one Dual Graphical User Interface

(GUI) workstation, and the Wide-Area Network (WAN) connection to the FAA Telecommunications Infrastructure (FTI) must be operating. Without the connections to either the Host Computer System (HCS) or the En Route Automation Modernization (ERAM) and Automated Radar Terminal System (ARTS) or Standard Terminal Automation Replacement System (STARS), necessary data will not be received by TBFM.

d. Since the local Ethernet LAN is not dependent on any one workstation being in operation, it can be seen that under normal conditions it is not necessary to shut down the entire local TBFM to perform maintenance or repair work.

e. Any one workstation may be taken out of service for diagnostic or replacement without necessitating a site shutdown. Certain processes (ARTS Data Interface (ADIF), Enhanced Traffic Management System (ETMS) Data Interface (EDIF), and GUI Router (GUIR)) are not redundant. Shutting down a workstation with one of these processes will result in the failure of that process.

1-13. Coordination.

a. Maximum availability is of prime importance to the users of FAA facilities, services, and equipment. Maintenance should therefore be accomplished, to the extent practicable, during periods of low activity, in coordination with the appropriate personnel. Much of the scheduled maintenance can be performed without interrupting operations.

b. SSC personnel shall thoroughly coordinate, in advance, with the site Air Traffic (AT) operations, any maintenance activity that may adversely affect the use of an operational facility. SSC personnel must be familiar with AT procedures to ensure that notification is made sufficiently early to allow AT personnel to take appropriate action. It is expected that AT personnel recognize the need for releasing equipment at the time scheduled for maintenance and cooperate in the furtherance of practices that assure continuous and reliable operation.

c. SSC personnel are responsible for keeping site AT personnel advised of the operational status of all systems, subsystems, facilities, and equipment. When unscheduled interruptions occur, prompt notification shall be made to site AT personnel. They shall be advised immediately when equipment fails, the system is operating in less than its redundant state, and when full service is restored.

1-14. Reliability Centered Maintenance.

a. Maintenance personnel shall follow the tasks and schedules provided in Chapter 4, which include the minimum essential Reliability Centered Maintenance (RCM) activities and the frequency with which they shall be performed to meet the minimum performance standards for the TBFM system.

b. The RCM program implements a mix of maintenance methods (periodic, Condition Based (CM), and Run-To-Fault (RTF) approaches) with the goal of achieving the required level of safety, reliability, and availability at the lowest cost.

1-15. – 1-99. Reserved.

DRAFT

Chapter 2. Technical Characteristics

2–1. Purpose. TBFM is a computerized decision support tool for air traffic controllers. TBFM is a time-based metering automation tool within the Center/Terminal Radar Approach Control (TRACON) Automation System (CTAS). TBFM provides benefits throughout the NAS, maximizing the use of available NAS resources, minimizing delays and disruptions to aircraft operators and their customers, as well as reducing fuel burn and engine emissions from reduced delays.

The TBFM system's mission is to efficiently utilize the available airport capacity without decreasing safety or increasing controller workload. The end users of TBFM are Traffic Management Coordinators (TMC) and controllers in ARTCCs, and TMCs in TRACONs and towers. The TMCs interact directly with the TBFM via display and input devices added into the Traffic Management Unit (TMU). The controllers interact indirectly with TBFM via the user interface on the En-Route or terminal Air Traffic Control (ATC) automation systems.

The system provides automation aids to assist in optimizing:

- The flow of traffic to adapted airports (i.e., airports for which adaptation data are available) within the ARTCC/TRACON;
- The flow of aircraft departing from an in-Center or in-TRACON airport destined for adapted airports;
- The use of the available runways and surrounding airspace; and
- The flow of aircraft in upstream Centers destined for adapted airports.

2–2. Description. The TBFM system consists of software processes, site adaptation, hardware processors, data storage devices, interface devices, and all associated cabling and connectivity hardware. TBFM software uses flight plan information, radar track data, weather forecast information, user settings and TBFM adaptation data to advise controllers on the sequencing, and scheduling of aircraft for the transition into terminal airspace and for en route departures. TMCs interact directly with the system via displays and input devices located in the TMU.

Each TBFM installation has workstation configurations consistent with the operational and support needs for the location. Key points are:

- a. Each ARTCC has its own hardware to run the full TBFM system. Each system is adapted for Metering Reference Elements (MRE) owned by that site (i.e., airports, fixes, departure points).
- b. Selected TRACONs and towers have a small subset of the full TBFM system, just enough to provide remote GUI displays from ARTCCs to those locations.

c. Each ARTCC acquires data from the external interfaces via FTI. This includes data from local and remote HCSs, ARTS/STARS, Traffic Flow Management System (TFMS), and CREWS.

Each ARTCC provides data to external interfaces via FTI. This includes Collaborate Arrival Planning (CAP) sent to VOLPE for use by Airline Operation Centers (AOC) and recorded data sent to Second Level Engineering (SLE) at the William J. Hughes Technical Center (WJHTC) for debug and test purposes. TBFM WAN connectivity is provided via FTI. The TBFM LAN requires WAN connectivity because it uses data from external systems. TBFM receives flight data from HCS or ERAM, ARTS (IIE, IIIE, IIIA), STARS, and TFMS. TBFM also receives weather data from the WJHTC. The WAN also provided connectivity between ARTCCs to support Adjacent Center Metering (ACM). See Figure 2–1, TBFM Wide Area Communications Network.

TBFM uses Cisco Routers to connect the TBFM Operational string and the TBFM Support string at the ARTCC. The routers also connect TBFM, via FTI, to remote TBFM GUIs in TRACONS and remote towers. A router at the TRACONS and remote towers complete the connectivity to the remote GUIs.

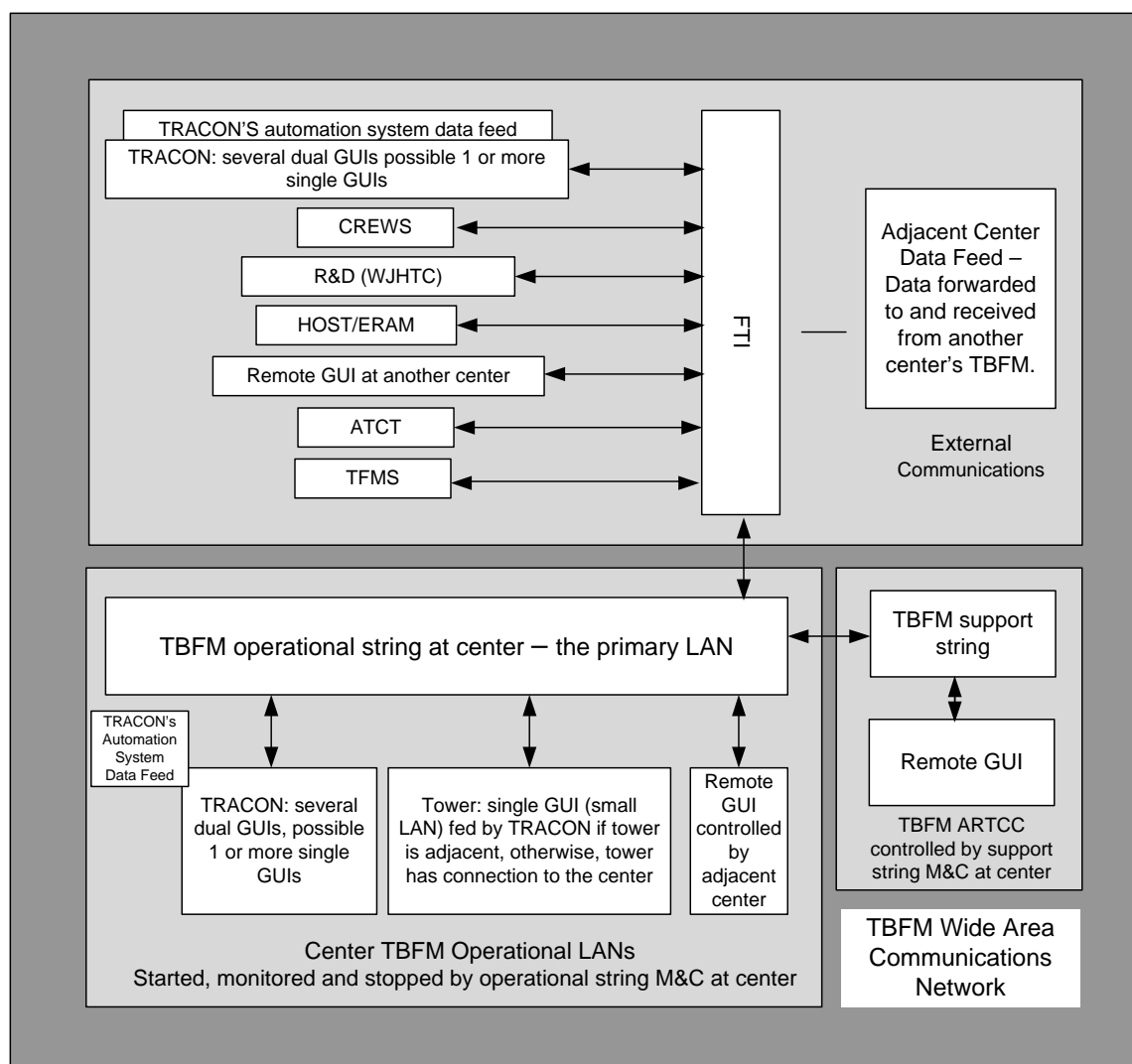


Figure 2–1. TBFM Wide Area Communications Network

NOTE: The router is the link to the WAN and without it, TBFM cannot complete its mission.

TBFM provides two main display views: a Timeline GUI (TGUI) and a Planview Graphical User Interface or geographic view (PGUI). These views provide the TMCs in the ARTCC TMU insight into traffic flow in the ARTCC area of interest. These views enable the TMCs to interpret the traffic flow situation and make strategic and tactical planning decisions to manage the flow. Through these GUIs, TMCs make inputs to the system to alter traffic flow and provide advisories to the En Route Air Traffic TMCs regarding these TMC changes. Estimated Time of Arrival (ETA) and STA timelines are produced and displayed by the TGUI.

2–3. Theory.

a. TBFM is a distributed processing system, using a number of workstations to share the processing workload, and connecting them through an Ethernet LAN.

b. The TBFM LAN has WAN connections to HCS or ERAM, ARTS, STARS, and TFMS, and to CTAS Remote Weather Service (CREWS). Access Control Lists, or filters, are defined on these interfaces to prevent unauthorized access to TBFM or through TBFM to HCS, ERAM, ARTS or STARS.

c. The TBFM M&C is a GUI that enables the user to start, stop, and configure TBFM processes. The M&C also provides real-time status for the TBFM hardware and system processes.

d. TBFM is comprised of two strings of workstations:

(1) An operational string for active use, and

(2) A support string for adaptation changes, testing of adaptations and software updates, and playback of flight data recorded from the operational string.

e. The TBFM software is a combination of COTS network management software with custom software modules written specifically for the TBFM application.

f. In addition to the programs that process flight data, TBFM software monitors the operation of TBFM itself. This software can automatically respond to error conditions.

g. TBFM operators use two types of GUI display:

(1) The TGUI shows AT as points along vertical lines. These indicate the time the aircraft will reach handoff or runway.

(a) Timelines can be set up to represent meter fix points or runways.

(b) Each operator can configure his or her display in a variety of ways to suit AT conditions and operator preferences.

(2) The second type of display used by TBFM operators is the PGUI. This shows a map view of AT in a manner similar to the Display System Replacement (DSR).

h. The Display Window Manager enables the TMC to dynamically start and stop any GUI for any adapted TRACON group on any display workstation. This consolidates the management of the display workstations and GUIs used by the ARTCC.

i. Information from TBFM may also be added to the data normally displayed on controller monitors.

2-4. Air Traffic Situations TBFM Addresses.

a. TBFM is an adjunct system to ATC that provides traffic flow data to assist traffic personnel in the development and execution of time-based metering initiatives in order to efficiently manage potential overcapacity situations.

b. ATCs in TRACONs must manage the flow of aircraft from the TRACON boundary to the runway threshold, with the same issues: increasing traffic density and workload.

c. TBFM calculates each aircraft's arrival/departure time and flight path. TBFM can also provide data on the TBFM GUI displays and on DSRs. These features allow ATM and ATC personnel to be relieved of some of the workload.

d. TBFM calculations of aircraft spacing and sequencing can improve safety and flow, and increase efficiency for runways.

e. TBFM shows continually updated calculations of aircraft position and path to allow TBFM and ATC personnel to better monitor the AT situation.

2-5. TBFM Software Processes.

a. TBFM software uses a complex set of processes working together in coordination to provide the calculations required.

b. The TBFM software processes are listed and described in paragraph 2-6(1) through 2-6(15).

(1) Communication Manager (CM).

(a) The CM process manages most of the other processes and all of the data calculation processes.

(b) CM accepts data through the Input Source Manager (ISM) process and assigns different processes of TBFM to accomplish the result of updating the PGUI and TGUI displays and DSR units.

(c) CM passes data from TGUI, PGUI, and DSR operators to HCS or ERAM.

(d) TBFM software processing is started when the M&C operator clicks on the appropriate icon on the M&C display.

(e) CM utilizes virtual machines for cm1 and cm2 (not actual workstations), running on the APP1 and APP2 servers. The virtual machine designated cm1 starts data processing when it receives instructions to do so from M&C, and continues to operate until it receives a signal from the M&C to shut down processing.

(f) The virtual machine designated cm2 also starts operation when M&C launches TBFM processing, but cm2 simply mirrors what is happening on cm1, so it can take over if cm1 fails.

(g) If cm1 fails, cm2 will automatically take over the CM functions.

(2) Host Data Interface (HDIF). HDIF is the process that interfaces TBFM and HCS/ERAM systems via the Host Interface Device (HID) NAS/Local Area Network (LAN) Host Air Traffic Management and Data Distribution System (HADDs), which maintains a database of current flight data received from the HCS. HDIF provides a one-way or two-way communication interface with HADDs.

(3) Input Source Manager (ISM).

(a) The ISM module listens on the network for data arriving from HDIF ADIF, and from adjacent ARTCC HADDS. ISM then alerts the CM process, which then handles assignment of processing tasks as required. ISM also mosaics the data from the HDIF, ADIF, and adjacent ARTCC HADDS data feeds.

(b) ISM runs on the active CM workstation.

(4) Dynamic Planner (DP).

(a) The DP assembles data from the various calculation programs in order to create schedules and runway allocations. While Route Analysis (RA) and Trajectory Synthesizer (TS) deal with individual aircraft, one at a time, DP must integrate their results to produce a schedule that has the aircraft reach the meter fix point or runway in an orderly stream.

(b) The DP module uses flight data from HCS/ERAM and the result of RA and TS calculations and weather data to calculate the optimum aircraft spacing and sequencing.

(c) Among the factors DP takes into account is aircraft size. (For example, spacing between aircraft should be increased when a small airliner follows a jumbo jet.)

(5) Route Analysis (RA).

(a) Whenever CM receives new data on a flight from HCS/ERAM, CM assigns an RA process to one of the RATS virtual machines (virtual machines for RATS1 and RATS2 run on the APP1 and APP2 servers).

(b) The RA process calculates the aircraft's route and ETA and returns the result to CM.

(6) Trajectory Synthesizer (TS). RA initiates and uses the data from TS to generate an ETA for each aircraft.

(7) Timeline GUI (TGUI). The TGUI displays the scheduling data provided by CM through DP and RATS.

(8) Planview GUI (PGUI). The PGUI displays graphical information provided by CM through ISM, RA, DP, and Weather Daemon (WDPD).

(9) ARTS Data Interface (ADIF). The ADIF is TBFM's interface with the TRACON's Automation System. ADIF receives flight and track data messages from the TRACON's Automation System, performs various processing on those messages, and forwards appropriate data to TBFM processes.

(10) Weather Data Processing Data (WDPD). The WDPD is responsible for receiving the Rapid Update Cycle (RUC) weather data file updates from the CREWS system at the WJHTC. It reformats and sends the updates to the GUIs, the CM, and the RATS.

(11) GUI Router (GUIR). The GUIR serves as a software multiplexer between the local CM process and multiple remote TBFM GUIs. The purpose of the GUIR is to reduce the volume of message traffic on the TBFM network between CM and the remote GUIs. The GUIR relieves CM of having to transmit the same message multiple times to remote GUIs. CM sends

one GUI message over the TBFM network to the GUIR, which in turn either broadcasts the message to all remote GUIs (all PGUIs/TGUIs), a remote GUI type (either all PGUIs or all TGUIs), or to a single identified GUI.

(12) Multifarious Universal Tester (MUT).

(a) MUT replays recorded TBFM binary message data for use with test, training, and troubleshooting.

(b) MUT connects to TBFM real-time processes under control from M&C, performs handshakes, and injects recorded binary message data to appropriate process(es) as determined by timing information obtained during data recording.

(13) Collaborative Arrival Planning (CAP). The CAP server process provides near real-time TBFM data to an external client. CAP is an optional process not essential to TBFM operation.

(14) Traffic Flow Management System (TFMS) Data Interface. The TFMS data interface accepts an incoming Extensible Markup Language (XML) data feed from TFMS that provides TBFM with flight plan and track data. This data is converted to internal TBFM formats and sent to ISM for association with other flight data. The TBFM M&C displays this process and icon as EDIF because the interface was developed when it was known as ETMS.

2-6. Monitor and Control (M&C).

- a. All control of TBFM is centered in the M&C function.
- b. The M&C controls the function of all the system's parts (including startup and shutdown, excluding TGUI and PGUI), monitors the health of all the system hardware and software, and is responsible for attempting to correct any system failures it detects.
- c. The M&C is composed of server and agent components used to monitor and command the TBFM system hardware and software, and a graphical user interface to provide users a mechanism to monitor and command the TBFM system.
- d. At an M&C position, M&C displays a banner containing "TBFM", the identification (ID) (Operational or Support), the current system release, and the Universal Time Coordinated (UTC). M&C updates the displayed time once per second.
- e. M&C displays the system string banner such that it cannot be overlaid by other display data. M&C also displays a menu of eligible commands from the system string banner via a right click.
- f. The M&C software allows the NAS Operations Manager (NOM) to configure, start, and stop TBFM processing. It monitors the system and the processing and provides alerts to the M&C if there is a problem.
- g. There are eight major clusters of status shown in the main window. These are the Control Room, Equipment Room, Engineering Support, External Interfaces, Services, Peripherals, Printers, and External Sites.

(1) The Control Room section lists all the equipment in the “upstairs” area, including all of the GUI workstations and M&C workstations.

(2) The Equipment Room section lists the physical and virtual servers needed to support the operational string.

(3) The Engineering Support section lists the physical and virtual servers needed to support the engineering support string.

(4) The Services cluster shows groups of software that make up a service to the system.

(5) External Interfaces shows the reported data interface status of the HCS/ERAM interfaces, as well as any TRACON and TFMS data interface status.

(6) The Peripherals section lists all the routers, switches, and other equipment.

(7) Printers are allocated their own cluster.

(8) The External Sites section lists the external facilities display workstations.

h. A system processor's availability status is an aggregate of the availability status of its address spaces and hardware components. The required address spaces depend on the operational role assigned to the system processor. The required hardware components depend on the processor type assigned to the system processor. Both of these assignments are accomplished with customization files.

i. For each system processor and devices, availability status includes up, degraded, manual intervention, and down. The statuses up, degraded and down reflect operational health from least severe to most severe. The status of manual intervention reflects a transition state.

j. M&C receives or derives notifications of significant system events. These events may include error occurrences, error recoveries, performance threshold trips, performance threshold recoveries, security events, and information events.

k. System events are subjected to filtering criteria to determine the criticality of each event. Four levels of criticality are available: Critical, Warning, Recovery, and Information. Color coding and other visual indicators are applied to each level of event. M&C applies the appropriate indicators and sends the events to the M&C Position's Events window. Critical and Warning events require acknowledgment (or auto acknowledgement) by the M&C position operator. Recovery and Information events do not require acknowledgment.

l. M&C may receive event notifications from other software products or may generate events itself based on conditions it detects. Though all events are available for display, the M&C position operator has the option to filter and/or sort the events to reduce workload. Each event that goes to the Events window is associated with a resource. The system resources that can provide events are Processor, Router, Switch, Printer, and External Interface.





m. Events are displayed with the date and time the event was detected, subject, resource and, if applicable, related component. For events associated with conditions outside the TBFM system, the subject is Interface; for events associated with a processor's software, hardware, or

functions, the subject is Processor and for events associated with a router port, a LAN switch, a LAN printer, the subject is Network.

(1) The Manage Event History Log function of M&C provides the support to search, display, and print a history of recent system events from the M&C position.

(2) System events consist of events (as presented in the Event Window), system command, system command feedback, or system command response events.

2-7. TBFM Error Handling and Recovery.

- a. TBFM uses the M&C software to monitor the status of the various processes.
- b. If a process fails, the software attempts to restart it.
- c. If one workstation fails in restarting a process, an alert message is sent to the M&C workstation to inform the M&C operator.
- d. If the attempt to assign the task to the alternate workstation fails, the M&C operator must intervene to manually resolve the problem.
- e. If a workstation or its network connection fails, the monitoring software on the M&C workstation alerts the M&C operator.
- f. If the primary router fails, the alternate router automatically takes over and an alert is sent to the M&C operator.
- g. Loss of data to the system is shown on the TGUI displays as a large red X on the screen.
- h. On the M&C display, icons represent hardware and processes. These icons indicate the status of the hardware or process as shown:
 - (1)  Up Status
 - (2)  Degraded Status
 - (3)  Down Status
 - (4)  Disabled

2-8. Red Hat Enterprise Linux (Release 6) Platform.

- a. TBFM uses the Red Hat Enterprise Linux Operating System (OS).
- b. An OS is the software that allows the workstation to start up and function.
- c. The Linux OS provides the capability to run virtual machines.
- d. It also supplies services such as printing, networking, keyboard and mouse handling, and low-level video support.

2–9. Hours of Operation.

a. TBFM software hours of operation may vary from site to site. Generally, TBFM software will be running during AT duty shifts. It may be shut down if no longer required by AT.

b. Software operation should be shut down from the active M&C console. M&C should not be shut down unless TBFM operation is shut down first.

2–10. TBFM Equipment Configuration. Refer to Figure 2–2, TBFM Configuration, with representative remote locations (TRACON and tower).

NOTE: Detailed information about the TBFM hardware components (workstation and rack descriptions, backup/restore, Light Emitting Diodes (LED), removal/replacement) is located in TI 6480.8, Section 4.

DRAFT

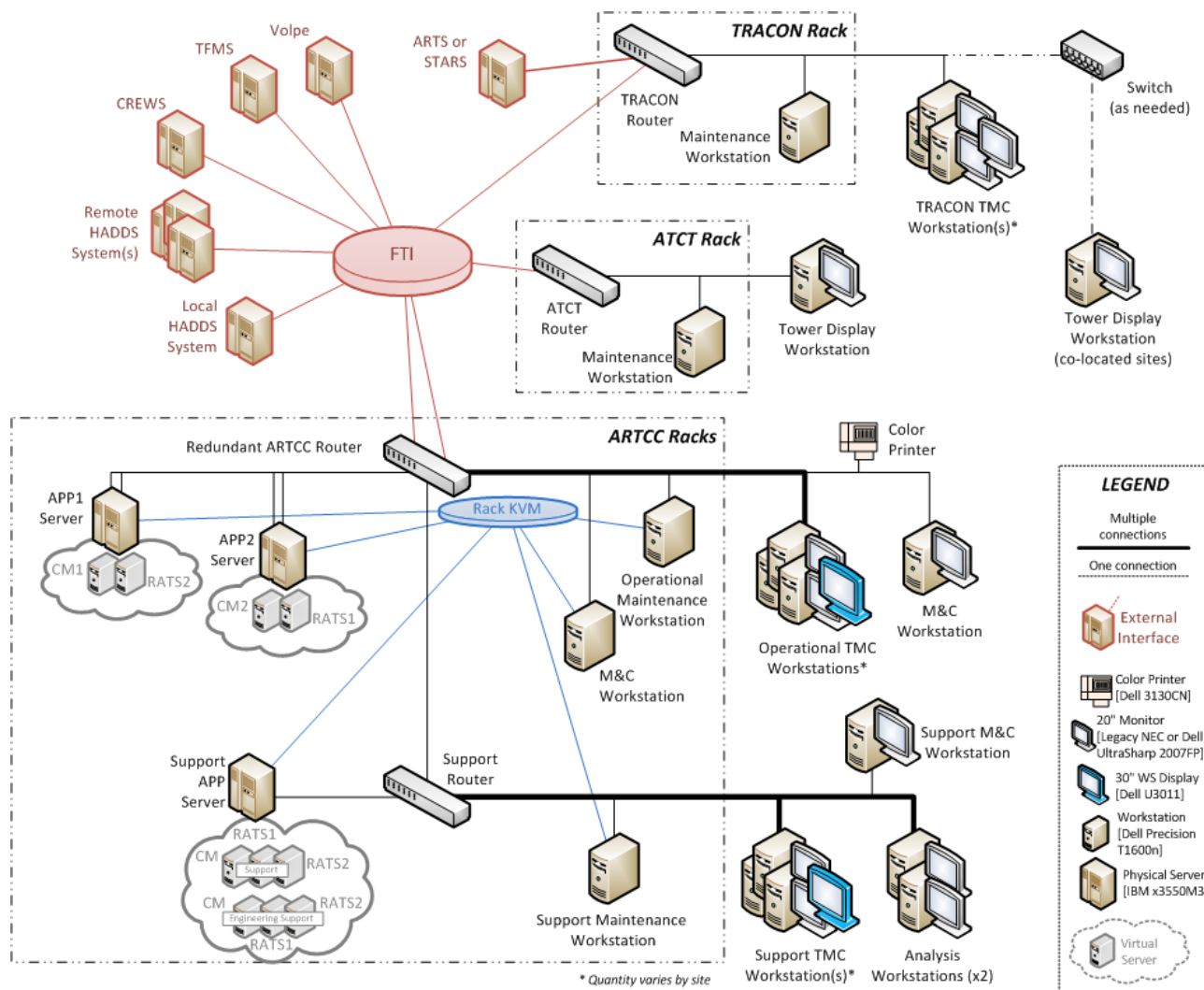


Figure 2-2. TBFM Configuration

2-11. TBFM Workstations

- a. TBFM uses the Dell Precision T1600n Linux workstation processors to provide high-speed computing capacity.
- b. There are several types of workstations used in TBFM. Each type is designed to accommodate specific TBFM tasks and to handle specific TBFM processing functions as follow.

(1) TMC Workstation. The TMC workstation is based upon the Dell Precision T1600n Linux workstation processor. This design applies to all TMC workstations, including the ARTCC, TRACON, ATCT and Air Traffic control Systems Command Center (ATCSCC), as the only difference between these workstations is the number and size of the displays. The workstation is supplied with a Universal Serial Bus (USB)-attached COTS keyboard and optical mouse. The workstation uses dual nVidia NVS 300 graphics adapters to support various combinations of legacy/new 20.1-inch and/or 30-inch monitors. The supported configurations are

determined by the COTS graphics adapter “dongle” used. Each dual-output dongle can support either dual (2) **DVI**-D or dual (2) DisplayPort digital video monitors (but not both on the same adapter).

(2) M&C Workstation. The M&C workstation is also based upon the Dell Precision T1600n Linux workstation processor. The M&C workstation is supplied with a USB-attached COTS keyboard and optical mouse. The M&C workstation uses one of its dual nVidia NVS 300 graphics adapters to support a single legacy or new 20.1-inch monitor using the supplied dual DVI-D adapter/dongle. The M&C workstation also includes a USB 2.0 speaker to provide audible alarms.

(3) Rack M&C Workstation. The Rack M&C workstations utilizes a Dell Precision T1600n workstation processor which is mounted on a slide-out shelf in the rack. The processor is attached to a monitor/keyboard/Keyboard/Video/Mouse (KVM) switch console mounted in a pull-out drawer. This assembly comes with a 17-inch diagonal Liquid Crystal Display (LCD) monitor which opens up to allow the user access to the keyboard and touchpad pointing device. The M&C workstation processor is connected to the rack-mounted monitor/keyboard/KVM assembly through a special Video Graphics Array (VGA)/USB cable provided with the monitor/keyboard/KVM switch assembly. This cable is attached to the KVM switch with an HD-15 connector and to the processor with a USB/VGA breakout at the other end. The VGA connector is attached to the dual DMS59-VGA adapter installed with the workstation processor.

(4) Analysis Workstation. The Analysis workstation is also based upon the Dell Precision T1600n Linux workstation processor. The Analysis workstation is supplied with a USB-attached COTS keyboard, and optical mouse. One of the two Analysis workstations is also supplied with a printer. The Analysis workstation uses one of its dual nVidia NVS 300 graphics adapters to support a single legacy/new 20.1-inch monitor using the supplied dual DVI-D.

(6) Maintenance Workstation. The Maintenance workstation utilizes a Dell Precision T1600n workstation processor which is mounted on a slide-out shelf in the rack in exactly the same manner as the M&C workstation. It’s user interface is provided by the rack-mounted monitor/keyboard/KVM switch console mounted in a pull-out drawer.

c. TBFM has a box-level replacement maintenance philosophy. This philosophy is designed to decrease outages and costs associated with workstation failure.

Table 2–1. TBFM Workstation Processes

Processor	Dell Precision T1600n Workstation	IBM System x3550 M3 Server
Type		
Processes		
M&C	X	
GUI	X	
DWM, GUIR, ADIF	X	
RATS (virtual machine)		X
HDIF, ISM, WDPD, CM (virtual machine), ADIF, DP, CAP, and EDIF		X
Analysis	X	
Backup Server (TBFM MWS)	X	

2–12. Dell Precision T1600n Processor.

a. The Dell Precision™ T1600n, shown in Figure 2–3, Dell Precision™ T1600n Processor, is a single-socket workstation. For the TBFM Maintenance workstations, operational/support TMC workstations, and operational/support M&C workstations, the Dell T1600n is equipped with one Intel® Xeon® E3-1225 quad-core processor operating at 3.10 Gigahertz (GHz), 4 Gigabyte (GB) 1333 MHz, non-ECC Random Access Memory (RAM) (2 x 2 GB DDR3 DIMMs), dual (2) 500 GB 7200 SATA hard disks, dual (2) nVidia® NVS 300 discrete graphics adapters, a 265W output power supply, and an integrated Gigabit Ethernet port. The Dell T1600n is a mini-tower form factor and is provided with a USB-attached keyboard and optical mouse. Each nVidia® NVS 300 PCIe graphics adapter is capable of supporting up to two (2) monitors at digital resolutions up to 2560 x 1600 pixels utilizing DisplayPort interface for a maximum of 4 monitors per workstation. Depending on function, there are up to four monitors connected, composed of combinations of 20.1-inch and 30-inch monitors connected to the graphics adapters. When used as the rack-mounted M&C workstation or Maintenance workstation, the workstation is connected to the rack-mounted monitor console and KVM switch through the USB and graphics ports. These attributes provide the processing power required by TBFM.

b. When a Dell Precision™ T1600n experiences a hardware failure, it should be replaced with a spare processor.



Figure 2–3. Dell Precision™ T1600n Processor

2–13. IBM x3550 M3 Server.

a. The IBM System x3550 M3, shown in Figure 2–4, IBM x3550 M3 Server, is a dual-socket processor. For the TBFM Application and Support Application servers, it is equipped with two Intel Xenon® E5645 six-core processors operating at 2.40 GHz, 24 GB (6 x 4 GB) 1333 MHz ECC RAM, dual (2) 500 GB 7200 Revolutions per Minute (RPM) hot-swappable hard disk drives, redundant hot-swap 460 watt (W) power supplies, and two integrated Gigabit Ethernet ports. The IBM x3550 is a 1 Rack Unit (RU) x 19" form factor which is slide-mounted and is provided with USB, DB-15 video (VGA), serial, and RJ-45 systems management ports. For TBFM, system management is accomplished through the USB and DB-15 video ports to a rack-mounted KVM switch with built-in monitor, keyboard, and pointing device (trackpad). Cooling is provided by six counter-rotating hot-swap fans with a built-in altimeter to control fan speed based upon atmospheric pressure.

b. The server functions to receive flight data and from it calculate aircraft arrival times, flight paths, sequencing, and spacing, and display the results to operators.



Figure 2–4. IBM x3550 M3 Server

2–14. Dell UltraSharp 2007FP Display.

a. TBFM data is displayed on the Dell UltraSharp 2007FP display, shown in Figure 2–5, Dell UltraSharp 2007FP Display. This monitor is used with the Operational and Support TMC workstations, Operational and Support M&C workstations, and Analysis workstations.

b. The Dell™ UltraSharp™ 2007FP 20.1-inch diagonal (20 inch viewable) Flat Panel LCD monitor provides resolution of up to 1600 x 1200 pixels (native) with contrast of up to 800:1 and brightness of 300 cd/m2. The monitor is provided with both analog (VGA) and digital (DVI-D) video interfaces. In all cases, the monitor is connected to the workstation using the digital (DVI-D) video interface. The monitor is provided with a tabletop stand that provides tilt, swivel, pivot (rotation) and height adjustments.



Figure 2–5. Dell UltraSharp 2007FP Display

2–15. Dell U3011 Display

a. TBFM data is displayed the Dell U3011 display. This monitor is used with the Operational TMC workstations.

b. The Dell™ UltraSharp™ U3011 30-inch diagonal Flat Panel LCD monitor shown in provides resolution of up to 2500 x 1600 pixels (native) with contrast of up to 1000:1 and brightness of 370 cd/m2. The monitor is provided with two HDMI (digital), 2 DVI-D (digital), 1 DisplayPort (digital), 1 VGA (analog), and component video (analog) interfaces. The monitor is connected to the workstation using the DisplayPort (digital) video interface. The monitor is provided with a tabletop stand that provides tilt, swivel, and height adjustments. The supplied stand does not support rotation. See Figure 2–6, Dell U301 Display.



Figure 2–6. Dell U3011 Display

2–16. NEC 20” Flat Panel Display (FPD).

a. TMA data is displayed on 20–inch NEC FPD. There are two display models in use: NEC LCD 2080UX+BK and NEC LCD 2090UXi-BK.

b. The NEC LCD 2080UX+BK has a 20.1–inch viewable area and is capable of resolutions up to 1600 x 1200 pixels at a refresh rate as high as 85 Hertz (Hz). See Figure 2–7, NEC LCD 2080UX+BK.



Figure 2–7. NEC LCD 2080UX+BK

c. The NEC LCD 2090UXi-BK has a 20.1–inch viewable area and is capable of resolutions up to 1600 x 1200 pixels at a refresh rate as high as 85 Hz. See Figure 2–8 , NEC LCD 2090UXi-BK.



Figure 2–8. NEC LCD 2090UXI-BK

NOTE: All ARTCCs use two 17-inch NEC (LCD1770NX+BK, LCD175M-BK, and LCD1770VX) FPD monitors (towers and TRACONs use one) for the rack mounted equipment. The monitor has a 17-inch viewable area and is capable of resolutions up to 1280x1024 pixels at a refresh rate as high as 75 Hz. One monitor is the rack mounted MC2 display and the second is rack mounted for the KVM switch.

2–17. RackMount RKP117-S801E Keyboard with KVM.

a. The RackMount Solutions RKP117e & CV-S801 is a 1U, 19-inch rack slide-mounted server console interface. It contains a 17-inch LCD color monitor (1280 x 1024 resolution), keyboard, touchpad, and 8-port KVM mounted in a pull-out drawer, and communicates with the rack-mounted servers and rack M&C workstation through VGA (HD-15) video and USB keyboard/mouse interfaces.

b. This server console and KVM switch are used by the maintainer to access the maintenance console interface on the servers and rack-mounted M&C workstation for setup, configuration, monitoring, and maintenance/troubleshooting. See Figure 2–9, Rack Mount Monitor, Keyboard, and Switch: RKP117-S801e.



Figure 2–9. Rack Mount Monitor, Keyboard, and Switch: RKP117-S801e

2–18. Printers.

a. The TBFM system utilizes two types of printers. The purpose of these printers is to provide hard copy printing capability for TBFM, for example, system logs and screen captures.

b. One network printer is connected to the TBFM system on the operational string. The network printer is a Dell 3130cn color printer.

c. The direct connect printer is connected to the Analysis workstation. The direct connect printer is a Hewlett Packard (HP) Officejet Pro 8000 Enterprise.

2–19. Dell 3130cn Color Printer. The Dell 3130cn, shown in Figure 2–10, Dell 3130cn Color Printer, is a tabletop color laser printer. It is attached to the operational or support LANs using an integrated 10/100 Ethernet port. It provides for general printing of reports or other documents as supported by the system software.



Figure 2–10. Dell 3130cn Color Printer

2–20. HP Officejet Pro 8000 Enterprise Printer. The HP Officejet Pro 8000 Enterprise, shown in Figure 2–11, Officejet Pro 8000 Enterprise Printer, is the printer used for the Analysis workstations.



Figure 2–11. Officejet Pro 8000 Enterprise Printer

2–21. Network Hardware.

a. Network connectivity for TBFM is handled by two routers and a switch (at some locations).

b. The standard TBFM network configuration includes:

- Cisco 2911/K9 router
- Cisco 3925/K9 router
- Cisco WS-C2960S-24TS-S switch

2–22. Cisco 2911/K9 Router.

a. The Cisco 2911/K9 router is an Integrated Services router with three onboard WAN or LAN ports, 16 total LAN ports and 0.5 GB of internal DDR2 memory. It also contains a single 210 W power supply and embedded hardware-based cryptography acceleration (IPSec + Secure Sockets Layer (SSL)). See Figure 2–12, Cisco 2911 /K9 Router.



Figure 2–12. Cisco 2911 /K9 Router

b. The purpose and function of the Cisco 2911/K9 router on TBFM is to link the TRACON and/or tower's Ethernet network to the ARTCC via the FTI network.

2–23. Cisco 3925/K9 Router.

a. The Cisco 3925/K9 router is an Integrated Services router with three onboard WAN or LAN ports, 36 total LAN ports (on redundant service modules installed in router) and 1 GB of internal DDR2 memory. It also contains dual 420 W power supplies and embedded hardware-based cryptography acceleration (IPSec + Secure Sockets Layer (SSL)). Figure 2–13, Cisco 3925 Router, shows the router.



Figure 2–13. Cisco 3925 Router

b. The purpose and function of the Cisco 3925 router on the TBFM operational string is to link the operational string with the support string router and the FTI network. FTI connectivity enables the operational and support strings to connect to all data feeds and remote facilities.

2–24. Cisco WS-C2960S-24TS-Switch.

a. The Cisco® Catalyst® WS-2960S-24TS-S shown in Figure 2–14, Cisco WS-C2960S-24TS-S Switch, is a Layer 2 fixed-configuration switch with 24 10/100/1000 Ethernet ports. The switch utilizes a GbE SFP (two are provided) uplink to connect to the TRACON router/switch.

b. This switch is used, as required, to provide extended LAN connections for devices in the TRACON or co-located ATCT that are more than 100 meters (328 feet) from the TRACON router/switch.



Figure 2–14. Cisco WS-C2960S-24TS-S Switch

2–25. Spectrum Controls AC SMARTStart® Switched Power Distribution Unit.

a. The Spectrum Controls AC SMARTStart® switched Power Distribution Unit (PDU) shown in Figure 2–15, Spectrum Controls AC SMARTStart® Switched Power Distribution Unit, is the power sequencer used in the racks. Power sequencers are used with the rack-mounted equipment for the following purposes:

- To provide an adequate number of receptacles for the equipment in the rack enclosure
- To provide redundant power connections in the ARTCC racks to feed the dual power supplies in the servers and routers
- To provide equipment-level circuit breaker and emergency power off protection
- To provide equipment-level transient protection
- To mitigate the effects of power-on inrush current in accordance with the applicable sections of FAA-G-2100H, Specification, Electronic Equipment, General Requirements.



Figure 2–15. Spectrum Controls AC SMARTStart® Switched Power Distribution Unit

2–26. TBFM Hardware Fault Isolation. The redundancy features, selection of the hardware used, and software monitoring combine to make hardware diagnosis in TBFM easier.

- a. The Monitor and Control software continually checks the status of workstations.
- b. The M&C workstation will alert the M&C operator to a detected failure. This enables the M&C operator to inform System Maintenance personnel of a specific fault, for example, RATS1 is down.

2–27. – 2–99. Reserved.

Chapter 3. TBFM Standards and Tolerances

3-1. General. Currently there are no essential standards and tolerances identified for the TBFM system. This chapter is reserved for future standards and tolerances that may be identified for TBFM. If any are identified, this chapter will list the essential system or equipment parameters, the standard value assigned to each parameter, and the initial and operating tolerances/limits imposed on each standard. Applicable components would be listed in the standards and tolerance table and, cross-referenced as appropriate to the paragraph that describes the procedures for checking each of the required parameters. Definitions that will apply are as follows:

- a.** The *Standard* shall be the optimum value assigned to an essential parameter of the system and shall be compatible with the system as a whole and the design capability of the equipment.
- b.** The *Initial Tolerance/Limit* shall be the maximum deviation from the standard value of the parameter, or the range, which is permissible when the system or equipment is accepted for use in the NAS at the time of initial commissioning or after any readjustment, modification, or modernization.
- c.** The *Operating Tolerance and Limit* shall be the maximum deviation from the standard value of the parameter or the range within which a system or equipment may continue to operate on a commissioned basis without adjustments or corrective maintenance and beyond which remedial action by maintenance personnel is mandatory.

STANDARDS AND TOLERANCES

<i>Parameter</i>	<i>Reference Paragraph</i>	<i>Standard</i>	<i>Tolerance/Limit</i>	
			<i>Initial</i>	<i>Operating</i>
3-2. – 3-99. RESERVED.				

NOTE: This table is reserved and will be populated if standards and tolerances are identified for TBFM.

DRAFT

Chapter 4. Maintenance Requirements

4-1. General. This chapter establishes all the maintenance activities that are required for TBFM on a periodic, recurring basis and the schedules for their accomplishment. The chapter is divided into two sections. The first identifies the performance checks (tests, measurements, and observations) of normal operating controls and functions, which are necessary to determine whether operation is within established tolerances/limits.

The second section identifies other tasks that are necessary to prevent deterioration and/or ensure reliable operation. All safety-related checks with direct impact to safety of flight within the NAS are clearly identified by a pound sign (#) placed to the left of the applicable task.

4-2. FAA Form 6000 Series. Order 6000.15 contains guidance and detailed instructions for field utilization of FAA Form 6000 series (Trend Analysis), as applicable to TBFM. Make entries in accordance with the instructions published in Order 6000.15 (except as otherwise instructed in the subparagraphs to follow). Forms are available at <http://tpr.faa.gov> and https://employees.faa.gov/tools_resources/forms/.

DRAFT

Section 1. Performance Checks		
Performance Checks	Reference Paragraph	
	Standards & Tolerances	Maintenance Procedures
4-1. OPERATIONAL AND SUPPORT WORKSTATIONS. Quarterly. Perform reboot	None	Par. 5-2
4-2. – 4-49. RESERVED.		

Section 2. Other Maintenance Tasks		
<i>Maintenance Tasks</i>	<i>Reference Paragraph</i>	
	<i>Standards & Tolerances</i>	<i>Maintenance Procedures</i>
4-50. TBFM EQUIPMENT. As Required.		
a. Clean air intake and exhaust vents	Visual	Par. 5-26
b. Clean cabinets.....	Visual	Par. 5-27
4-51. MONITORS. As Required.		
a. Adjust FPD monitor	Visual	Par. 5-28
b. Clean FPD monitor	Visual	Par. 5-29
4-52. PRINTERS. As Required.		
Clean printers	Visual	Par. 5-30
4-53. – 4-75. RESERVED.		

Section 3. Special Maintenance Procedures		
<i>Maintenance Tasks</i>	<i>Reference Paragraph</i>	
	<i>Standards & Tolerances</i>	<i>Maintenance Procedures</i>
4-76. WORKSTATIONS. Dell T1600n Processor Replacement	None	TI 6480.8, section 4 Par. 4.8.4
4-77. CISCO ROUTERS. a. Cisco 2911 Router Restoration	None	TI 6480.8, section 4 Par. 4.4.4
b. Cisco 3925 Router Restoration		Par. 4.5.4
c. Cisco 2960 Switch Restoration		Par. 4.6.4
4-78. MONITORS. a. Dell U3011 Display Replacement	None	TI 6480.8, section 4 Par. 4.11.3
b. Dell 2007FP Display Replacement		Par. 4.12.3
c. NEC 20" LCD Monitor Replacement.....	None	TBD
4-79. PRINTERS. a. Dell 3130 Color Printer Replacement	None	TI 6480.8, section 4 Par. 4.9.3
b. Officejet Pro 8000 Enterprise Printer Replacement		Par. 4.10.3
4-80. KVM. RackMount RKP117S801e Keyboard with KVM Replacement	None	TI 6480.8, section 4 Par. 4.13.3
4-81. APPLICATION SERVERS. IBM x3550 M3 Server Replacement	None	TI 6480.8, section 4 Par. 4.7.4
4-81. RACK POWER DISTRIBUTION. Spectrum Controls Switched Power Distribution Unit Replacement	None	TI 6480.8, section 4 Par. 4.14.3
4-83. – 4-99. RESERVED.	None	

Chapter 5. Maintenance Procedures

5-1. General.

a. This chapter establishes the procedures for accomplishing the various essential maintenance activities that are required for the TBFM system on either a periodic or incidental basis. The chapter is divided into two sections. The first section describes the procedures to be used in making the performance checks listed in chapter 4, section 1, of this handbook. The second section describes the procedures for doing the tasks listed in chapter 4, section 2, of this handbook.

b. Refer to the latest edition of Order 6000.15 for additional general guidance. Only those procedures not in the equipment instruction books are specified herein.

c. Maintenance procedures shall be performed under conditions that duplicate, as closely as practicable, those present during normal operation.

DRAFT

Section 1. Performance Check Procedures

5-2. Reboot Operational and Support Workstations.

a. Objective. These tasks clear out memory leaks and stray processes if they exist, and remove accumulated temporary files. Upon reboot, all workstations should return to service, in effect, with a clean slate, able to function at optimum performance.

b. Discussion. These tasks should be performed at a time when the TMU and support string users do not need the use of the system.

c. Test Equipment Required. None.

d. Conditions. This test must be performed at a time of low activity at the site, to avoid interfering with TMU operations.

e. Reboot Manager. Refer to TI 6480.8, Section 8.5, TBFM Reboot Manager.

NOTE: This procedure should be performed during off-peak traffic hours because TBFM will have to be shut down for approximately 15 minutes while the workstations reboot. All workstations that have been shut down with the rebootManager will have to be powered back on by pressing the power button on the workstation. This will require coordination with personnel at remote facilities (i.e., TRACON, Tower, or adjacent centers.)

(1) From the M&C workstation shut down TBFM.

(2) Reboot all TBFM workstations by powering down the processor, wait about ten seconds, and then power up the processor.

(3) After all workstations reboot, log in to the M&C workstation and restart TBFM.

5-3. – 5.25. Reserved.

Section 2. Other Maintenance Task Procedures

5–26. Clean Air Intake and Exhaust Vents.

a. Objective. To provide maximum cooling ventilation to the TBFM system components that require air circulation. Components include workstations, routers, and monitors.

b. Discussion. Electronic devices are prone to premature failure because of heat if the cooling airflow is disrupted or restricted. Dust, dirt, and carpet pile can block the air flow. Periodic cleaning will ensure constant airflow to the TBFM system component internals.

c. Test Equipment Required: None.

d. Conditions. Dirty input and exhaust fan vents or convection airflow slots.

e. Detailed Procedure. Use a portable vacuum cleaner hose, preferably with a brush attachment. Vacuum all air intake and exhaust ports. Vacuum all slots in housings designed to accommodate convection air currents. An example of such openings is the slots in the sides and top of the monitor housing.

5–27. Clean Dirty Cabinets.

NOTE: This procedure applies to all TBFM equipment cabinets.

a. Objective. To remove unsightly grime, pencil and pen marks, dirt, and other types of discoloration caused by usage from the cabinets.

b. Discussion. Equipment housings tend to become dirty. Extended use of a keyboard causes accumulation of soil marks from the hands. Movement of a hand holding a pencil may cause a mark on the monitor if the pencil touches the housing. The equipment can take on an unsightly appearance if dirt has accumulated and the equipment has not been cleaned.

c. Cleaning Equipment Required. A pan of water and a soft rag or cloth are required. If the grime is difficult to remove a mild cleaning agent such as a detergent or liquid cleaner may be required.

d. Conditions. Unsightly appearance of equipment.

e. Detailed Procedure.

- (1) Assemble the cleaning materials. Dampen the cloth or rag with the cleaning agent.
- (2) Wipe the cabinets with the dampened cloth or rag.
- (3) Be careful not to spill water or a liquid cleaning agent down into the keyboard.

5–28. Adjust FPD Monitor Controls.

a. Objective. To maintain the FPD at their peak performance as they age.

b. Discussion. On initial setup and as the FPD ages, the picture presented on the screen may not be optimal. The most common adjustments that may be required are brightness, contrast, and image size.

CAUTION: Do not bring magnetized materials or objects that give off a magnetic field into close proximity to the FPD. An example of a device that generates a surrounding magnetic field can be a pencil sharpener.

c. Test Equipment Required. None required for routine field maintenance.

d. Conditions. If deterioration in FPD performance becomes noticeable, such as inadequate brightness or contrast, adjustment may alleviate the symptoms. Using the auto adjust function or moving the adjustment control through its dynamic range (limits) can establish where the best setting exists.

e. Detailed Procedures. None.

5–29. Clean FPD Monitor.

a. Objective. To remove dust, dirt, grime, and finger marks from the viewing panels of the FPD.

b. Discussion. The viewing panel tends to accumulate dust and grime over time. This can reduce brightness and clarity and become a distraction to those who use the monitor.

c. Cleaning Equipment Required. Only a soft cloth dampened with water should be used on the display. No cleaning agents should ever be used on the plastic panels.

d. Conditions. Dirty monitor viewing panel.

e. Detailed Procedure.

(1) Unplug the FPD from the power outlet before cleaning.

(2) To clean the FPD screen, lightly dampen a soft clean cloth with water. If possible, use a special screen cleaning tissue or solution suitable for the antistatic coating.

(3) To clean the FPD cabinet, use a cloth lightly dampened with water.

CAUTION: Never use flammable cleaning material to clean the FPD or any other electrical apparatus.

5–30. Clean Printers.

a. Objective. To maintain optimal printer quality by cleaning the printer and where applicable aligning the printheads.

b. Discussion. Printers can become clogged with paper, toner, or dust particles over time, causing print quality to degrade.

c. Cleaning Equipment Required. Refer to individual printer's cleaning procedures for required cleaning equipment.

d. Conditions. Print quality is degraded through buildup of dust particles.

e. Detailed Procedure. Select the site printer's cleaning procedure from the following printers:

NOTE: The printer manuals can be located under Software/Hardware Documents on the NASE portal's TBFM community located at <https://www.nase.faa.gov> (internet users) or <https://nase.amc.faa.gov> (intranet users).

(1) Dell 3130cn Color Printer. No documentation on cleaning in the Dell 3130cn Color Printer User Guide.

(2) HP Officejet Pro 8000 Enterprise Printer. The HP Officejet Pro 8000 Enterprise User's Manual provides instructions on cleaning the printheads. Refer to Section 4, Solve A Problem, and the subsection titled To Clean the printheads.

DRAFT

Section 3. Special Maintenance Task Procedures

5-31. General. All special maintenance procedures for TBFM are contained in TI 6480.8.

5-32. – 5.99. Reserved.

DRAFT

Chapter 6. Flight Inspection

6-1. – 6.99. Reserved.

DRAFT

This page intentionally left blank.

Appendix 1. List of Acronyms and Abbreviations

Abbreviations	Definitions
ACM	Adjacent Center Metering
ADIF	ARTS Data Interface
AJW	Technical Operations (organization)
AOC	Airline Operation Centers
ARTCC	Air Route Traffic Control Center
ARTS	Automated Radar Terminal System
AT	Air Traffic
ATA	Advanced Technology Attachment
ATC	Air Traffic Controller
ATM	Air Traffic Management
ATO	Air Traffic Organization
BIOS	Basic Input/Output System
CAP	Collaborative Arrival Planning
CCD	Configuration Control Decision
CM	Configuration Management
CM	Communications Manager
CONUS	Continental United States
COTS	Commercial Off-the-Shelf
CREWS	CTAS Remote Weather Service
CTAS	Center TRACON Automation System
DDR	
DHS	Department of Homeland Security
DIMM	
DOT	Department of Transportation
DP	Dynamic Planner
DSR	Display System Replacement

Abbreviations	Definitions
DVI	
ECC	
EDIF	ETMS Data Interface
ERAM	En Route Automation Modernization
ETA	Estimated Time of Arrival
ETMS	Enhanced Traffic Management System
FAA	Federal Aviation Administration
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FPD	Flat Panel Display
FTI	FAA Telecommunication Infrastructure
GB	Gigabyte (10 ⁹)
GHz	GigaHertz
GUI	Graphical User Interface
GUIR	GUI Router
HADDS	Host/Air Traffic Management and Data Distribution System
HCS	Host Computer System
HDIF	Host Data Interface
HID	Host Interface Device
HP	Hewlett Packard
HNL	HID/NAS LAN
Host	see HCS (ARTCC ATC)
IAW	In Accordance With
ID	Identification
IDE	Integrated Drive Electronics
ISM	Input Source Manager
ISSO	Information Systems Security Officer
KVM	Keyboard, Video, Mouse switch

Abbreviations	Definitions
LAN	Local Area Network
LCD	Liquid Crystal Display
LED	Light Emitting Diode
LES	Law Enforcement Sensitive
M&C	Monitor and Control
MB	Megabyte (10^6)
MHz	Megahertz
MRE	Metering Reference Elements
MTHB	Maintenance Technical Handbook
MUT	Multifarious Universal Tester
NAS	National Airspace System
NASE	NAS Environment
NCP	NAS Change Proposal
NOM	NAS Operations Manager
NSA	National Security Agency
OS	Operating System
OUO	Official Use Only
PCII	Protected Critical Infrastructure Information
PDF	Portable Document File
PGUI	Planview Graphical User Interface
RA	Route Analysis
RAM	Random Access Memory
RATS	Route Analyzer/Trajectory Synthesizer
RJ	
ROM	Read Only Memory
RPM	Revolution per minute
RTF	Run-to-Fault
RUC	Rapid Update Cycle

Abbreviations	Definitions
SATA	
SBU	Sensitive But Unclassified
SCAP	Security Certification and Authorization Package
SCSI	Small Computer System Interface
SHSI	Sensitive Homeland Security Information
SSC	System Support Center
SSI	Sensitive Security Information
STA	
STARS	Standard Terminal Automation Replacement System
SUI	Sensitive Unclassified Information
TBFM	Time Based Flow Management
TFMS	Traffic Flow Management System
TGUI	Timeline Graphical User Interface
TMC	Traffic Management Coordinator
TMU	Traffic Management Unit
TOARR	Technical Operations Aircraft Accident Representative
TRACON	Terminal Radar Approach Control
TS	Trajectory Synthesizer
TX	Transmit
USB	Universal Serial Bus
UTC	Universal Time Coordinated
VGA	Video Graphics Array
WAN	Wide Area Network
WDPD	Weather Daemon
WJHTC	William J. Hughes Technical Center
XML	Extensible Markup Language

Appendix 2. Policy/Procedures for Identifying, Handling, Marking and Disposal of Sensitive Unclassified Information (SUI)

A2-1. Purpose. This appendix provides guidance to employees regarding the rules and practices for identification, handling, marking, storage and disposal of media that contains For Official Use Only (FOUO) information, Sensitive Security Information (SSI), Sensitive Homeland Security Information (SHSI) and/or Protected Critical Infrastructure Information (PCII). This guidance does not pertain to any Classified (i.e., Confidential, Secret, and Top Secret) media.

This appendix provides guidance to employees regarding the rules and practices for identification, handling, marking, storage and disposal of media that contains For Official Use Only (FOUO) information, Sensitive Security Information (SSI), Sensitive Homeland Security Information (SHSI) and/or Protected Critical Infrastructure Information (PCII). This guidance does not pertain to any Classified (i.e., Confidential, Secret, and Top Secret) media.

A2-2. Scope. This guidance pertains to any SUI discussed verbally, transmitted electronically, existent or generated as printed material and/or contained on hard drives, disk drives, and/or any other type of computer storage media under the purview of the FAA. It pertains to every FAA employee, contractor, consultant and grantee creating, handling, or accessing SUI.

A2-3. Background. In the aftermath of September 11, 2001, there is a heightened awareness of the need to safeguard sensitive Government information that does not meet the standards for classified national security information. Of particular concern is the need to protect Government information related to homeland security. This includes information that supports the FAA global aerospace structure that contributes to the security of the nation and public safety. It is incumbent upon all FAA associated personnel to support these safeguards through increased awareness of the nature of such material and their duties and responsibilities for its protection.

A2-4. Policy. In Accordance With (IAW) requirements stated in the latest edition of Order 1600.75, Protecting Sensitive Unclassified Information (SUI), SUI is unclassified information — in any form including print, electronic, visual, or aural forms — that must be protected from uncontrolled release to persons outside the FAA and indiscriminate dissemination within the FAA. It includes aviation security, homeland security, and protected critical infrastructure information. SUI may include information that may qualify for withholding from the public under the Freedom of Information Act (FOIA). All personnel shall be aware of and follow the policies and procedures contained herein and in the latest edition of Order 1600.75. If conflicting guidance is provided, comply with Order 1600.75.

A2-5. Types of SUI. Throughout the Federal Government there are more than 50 types of SUI. Within the FAA, only four types are generally encountered or handled:

a. FOUO Information. FOUO is the primary designation given to SUI by the Department of Transportation (DOT) and FAA. It consists of information that could adversely affect the national interest, the conduct of Federal programs, or the privacy of individuals if released to unauthorized individuals. As examples, the uncontrolled use of FOUO information may allow someone to:

(1) Circumvent agency laws, regulations, legal standards, or security protective measures

or

(2) Obtain unauthorized access to an information system.

b. SSI. SSI is a designation unique to the DOT and DOT's operating administrations and to the Department of Homeland Security (DHS). It applies to information we obtain or develop while conducting security activities, including research and development activities. Unauthorized disclosure of SSI would:

(1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file);

(2) Reveal trade secrets or privileged or confidential information obtained from any person;

or

(3) Be detrimental to transportation safety or security.

c. SHSI. SHSI is a designation unique to homeland security information that we share with State and local personnel. The Federal Government shares SHSI with State and local personnel who are involved in prevention against, preparation for, or response to terrorism. We protect it because its loss, misuse, unauthorized disclosure or access, or modification can significantly impair the capabilities and efforts of Federal, State, and local personnel to predict, analyze, investigate, deter, prevent, protect against, mitigate the effects of, or recover from acts of terrorism. If our sensitive unclassified information impairs these capabilities, we must designate it SHSI before we share it with State and local personnel to facilitate its proper protection.

d. PCII. PCII is a designation unique to critical infrastructure information provided by non-government persons and entities to the DHS. DHS uses the information for security of critical infrastructure and protected systems, analysis, warning, interdependency studies, recovery, reconstitution, or other informational purposes. While only DHS can designate information as PCII, they can share it with other Federal agencies as needed for operational purposes. PCII is defined in 6 CFR Part 29.1.

A2-6. Identifying and Working With SUI. Personnel working with this system are most likely to encounter SUI identified above. However, other Federal agencies use different terminology and markings to designate SUI. For example, the Department of Energy uses Official Use Only (OUO), the Department of State uses Sensitive But Unclassified (SBU), and the Drug Enforcement Administration uses DEA Sensitive. Many Federal law enforcement agencies use the term Law Enforcement Sensitive (LES). If an unfamiliar security designation is encountered, contact the SSE for guidance; treat the information in question as FOUO until specific resolution is obtained.

Most existent SUI will be marked accordingly. However, marking is not conclusive proof of sensitivity. Information sensitivity may cease because of the passage of time or change in circumstances. Also, because of error or changing sensitivities, unmarked SUI that should be

marked or information that is marked but is no longer sensitive may be encountered. If there is any uncertainty about markings, contact the supporting SSE for a resolution and protect the questioned information as though it were FOUO information pending resolution.

The systems under cognizance of the Communications, En Route Peripheral Support Group, their operating systems and operational and backup data typically fall outside the scope of designation as SUI. However, the following specific information associated with the En Route Peripheral Support Group programs and systems is considered SUI:

- a. Lists and/or data files of employees and their respective system passwords or access codes. (FOUO)
- b. System specific security information. (FOUO)
- c. System or organizational vulnerability assessments. (SSI)
- d. Continuity of Operations Plan (COOP) documentation. (SSI)
- e. Security Certification and Authorization Package (SCAP) documentation. (SSI)
- f. Contingency planning documents, such as Disaster Recovery Plans. (SSI)
- g. Trade secret or proprietary corporate information supplied in proposals and/or provided to the FAA under contract license agreements. (SSI).

A comprehensive, but generic listing of the specific information comprising SSI is provided in Order 1600.75, appendix A.

A2-7. Marking/Labeling SUI. Marking is a basic protective measure that draws a reader's attention to the sensitivity of information and the need to protect it. Marking aids in making disclosure decisions and selecting and applying appropriate protective measures.

All personnel are required to properly mark information when created or it is determined that it meets the standards of sensitive unclassified information. Exceptions:

- a. **Records in storage.** If there are unmarked records in storage that should be marked, they need not be removed from storage only to mark them. Mark them when removed from storage for other purposes other than destruction. Stored documents slated for destruction need not be marked prior to destruction provided the individual removing the document from storage can ensure destruction is accomplished as specified in paragraph 10 of this appendix.
- b. **Records marked under old authority.** Information marked under an old regulatory authority, e.g., 14 CFR § 191 for Sensitive Security Information may be marked differently than directed by this order. Remarketing these documents is not required.
- c. **Sensitive non-government information.** Your office may receive information from contractors, grantees, businesses, and regulated parties marked as business sensitive, company confidential, proprietary, trade secret, and so on. Remarketing this information is not required, but it must be protected from unauthorized disclosure. Unless greater protective measures are specified by the information's originator, protect it as FOUO information.

Refer to Order 1600.75, appendices D and E, for the most current guidance for marking FOUO information and SSI, which have different marking protocols. The SHSI Program Officer and PCII Officer will issue separate marking guidance for SHSI and PCII.

When marking documents and other material containing both classified national security information and SUI, refer to the latest edition of Order 1600.2, Safeguarding Controls and Procedures for Classified National Security Information and Sensitive Unclassified Information.

Mark other records, such as photographs, films, tapes, slides, or records residing in information systems with appropriate protective markings and distribution limitation statements in a conspicuous way so that persons having access to them are aware of their sensitivity.

Mark removable electronic media, e.g., diskettes and compact disks, with the appropriate protective marking and distribution limitation statement in a conspicuous way so that persons having access to them are aware of their sensitivity. The System ISSP will contain additional specific measures for labeling and marking removable media.

A2-8. Storing SUI.

a. During Working Hours.

(1) **Physical custody or control.** When SUI is not in secure storage, it must be under the protection and control of an authorized person.

(2) **Not under physical custody or control.** When your SUI is not under the physical custody or control of an authorized person, you must store it in a lockable container, such as a file cabinet or desk, or in a locked space. Your office must control the keys to the locks of these containers and spaces, and key holders must be authorized persons.

b. After Working Hours.

(1) **Uncontrolled work spaces.** If the work area is accessible to persons, who are not authorized access to the SUI, it must be stored in a secure container such as a locked desk, file cabinet, or an inaccessible locked space. The sub-team office must control the keys to the locks of these containers and spaces, and key holders must be authorized persons.

(2) **Controlled work spaces.** If the work area is accessible only to persons who are authorized access to the SUI, additional protective measures are not needed. Again, the sub-team office must control the keys to the locks for these controlled workspaces.

c. At Home or On Travel. Working on SUI outside the workplace poses additional security risks and challenges. If there is a need to work with SUI at home or while on travel, the system manager's approval to do so must be obtained. Each individual holder of SUI is responsible for protecting it from unauthorized disclosure while at home or traveling. Whether working and storing SUI from home or an assigned travel destination, the information is to be provided the same level of protection that it is afforded at the normal work site.

A2-9. Distribution Procedures for SUI. SUI may be carried, mailed, or shipped in any manner that prevents inadvertent disclosure of the contents. When sending SUI records outside the DOT, include supplementary markings and notices to explain the significance of the

information and promote its proper handling. For example, include a statement such as the following in a transmittal record or directly on the record containing SUI:

This document/record belongs to the Federal Aviation Administration and may be used for official government purposes only. It may not be released without the express permission of the Federal Aviation Administration. Refer requests for the document to:

(insert name and address of originating office.)

a. Hand carrying. Place the information in an opaque envelope or carry it within a brief case, pad folio, or other container. For FOUO information, use DOT Form 1600.7-1, FOUO Cover Sheet, or the FAA Form 1360-39, FOUO Envelope, if available.

b. Interoffice mail. Use a sealed opaque envelope with the addressee indicated on it. This is in addition to or instead of any office messenger envelopes. If available, use FAA Form 1360-39.

c. U.S. or Contract Mail. Mail or send documents and materials in properly addressed opaque envelopes or containers by United States Postal Service first-class, certified, or registered mail or contracted delivery service. Bulk shipments, such as directives, may be sent by 'fourth-class' mail provided the shipment is wrapped in opaque covering.

d. Telephone. Confirm that you are speaking to an authorized person before discussing the information, and inform the person that your discussion will include SUI and what part of the discussion is sensitive. Never leave voicemail messages containing SUI.

e. Fax.

(1) Mark the fax. Ensure that the documents being faxed are appropriately marked;

(2) Send to correct number. Use special care to ensure that documents are being sent to the correct fax number; and

(3) Determine how faxes are handled at the receiving end:

(a) If sending the fax to a controlled area, where only authorized persons will have access to it, then it may be sent without further precautions.

(b) If sending the fax to an uncontrolled area, where unauthorized persons might have access to it, then request an authorized person stand by at the receiving end while the fax is being sent. Ask for a confirming receipt.

f. Electronic Mail. Mark emails in the subject line "For Official Use Only" or "Sensitive Security Information" as appropriate. Send sensitive unclassified information as attachments; ensure they are appropriately marked IAW Order 1600.75, appendices D and E. Also, the security and encryption procedures of Order 1370.81, Electronic Mail Policy, must be followed.

g. Web Sites. Posting SUI to an unsecured website that can be accessed by the public from the Internet is prohibited. Public web sites must not be provided links to web sites where SUI is posted. SUI may be posted to restricted FAA web sites provided they have special logon protocols and password protection. Passwords to these sites may be provided only to persons who satisfy the "duty to protect" and "need-to-know" requirements explained in Order 1600.75.

A2-10. Disposal of SUI. The following guidance is provided for paper documents and record IAW requirements stated in Order 1600.75. Refer to the current version of this order to ensure this information is current.

Destruction Standards for Paper Documents and Records		
If your document is:	Then your destruction standard is	Method
FOUO	To make recognition and reconstruction difficult	At a minimum, tearing or shredding each page into small pieces and mixing those pieces into regular trash
SSI	Completely to preclude recognition or reconstruction	Burning, shredding, wet-pulping and chemical decomposition (Note 1)
SHSI	By any means approved for destruction of classified information or by any other means that would make it difficult to recognize or reconstruct the information	Burning, cross-cut shredding, wet-pulping and chemical decomposition
PCII	By any method that prevents unauthorized retrieval	Burning, cross-cut shredding, wet-pulping and chemical decomposition
NOTE: Existing strip shredders may be used, but cross-cut shredding is preferred. Any new shredding equipment must have a cross-cut feature. The local Servicing Security Element (SSE) can provide assistance in selecting an appropriate destruction method and equipment.		

Refer to Appendix 3, Sensitive Security Information and Magnetic Media Disposal/Reutilization Policy/Procedures, for guidance pertaining to electronic/computer storage media.

Appendix 3. Sensitive Security Information and Magnetic Media Disposal/Reutilization Policy/Procedures

A3-1. Purpose. This appendix provides guidance to Technical Operations Services (TOS) employees who have a requirement to dispose of, or reuse, unclassified computer storage media that contains Sensitive Security Information (SSI) or For Official Use Only (FOUO) information. These procedures do not pertain to any Classified (i.e., Secret, Top Secret) media.

A3-2. Scope. These procedures pertain to any Sensitive but Unclassified (SBU) data contained on hard drives, disk drives, and any other type of computer storage media under the purview of the Federal Aviation Administration (FAA) that contains SSI or FOUO information. Computer storage media located at FAA site(s), but owned or managed by other government agencies (i.e., Department of Defense (DoD), Federal Bureau of Investigation (FBI)), will not use these procedures, but will follow the procedures and/or guidelines for reusing or destroying magnetic media dictated by that particular agency. If the storage media is FAA-owned but contains sensitive information from another outside agency (i.e., DoD), then the sanitization procedures from the outside agency must be followed. If the outside agency's procedures are determined by the division Information Systems Security Officer (ISSO) to be better than or equal to the procedures outlined in this appendix, then no other action is necessary. If the outside agency's procedures are unknown or less stringent, then the procedures outlined in this appendix should be utilized.

A3-3. Background. Computer storage media that contains SBU information cannot be reused or excessed unless all information has been destroyed or removed beyond comprehension. Reformatting the drive or deleting files will not completely remove the data from a system. There is still a great chance that the data can be recovered.

A number of methods can be used to accomplish proper sanitization. This document will provide three sets of procedures that will satisfy requirements necessary for reusing or disposing of electronic storage media. These procedures are:

- a. overwriting the data manually and/or using approved data-overwriting software,
- b. degaussing (i.e., demagnetizing the data), and
- c. destroying the media.

A3-4. Policy. In accordance with requirements stated in the latest edition of Order 1370.82, Information Systems Security Program, to maintain the confidentiality and accountability of sensitive information, TOS FAA and support contractor personnel shall ensure confidentiality of sensitive data when reusing or disposing of magnetic media. The procedures contained in this document shall be followed when disposing of, or reusing, unclassified computer storage media that contains SSI and/or FOUO information. Authority to destroy magnetic media must be obtained from the owner or Property Custodian, whichever is appropriate, prior to executing any procedure that destroys data or the media.

All personnel shall follow the latest edition of Order 1600.2, Safeguarding Controls and Procedures for Classified National Security Information and Sensitive Unclassified Information, when disposing or reusing magnetic media that contains classified information.

A3-5. Procedures for Sanitizing SBU Electronic Storage Media. Any one of the following procedures can be used when sanitizing any SBU electronic storage media before reuse or disposal. Before SBU media is to be removed or reused, the Division ISSO must be notified and consulted.

a. Overwriting Electronic Storage Media for Sanitization.

Overwriting is the process of replacing information (data) with meaningless data in such a way that the meaningful information cannot be recovered. The individual performing the overwriting will be responsible for certifying that the process has been successfully completed.

The process of overwriting data must be correctly understood and carefully implemented to be effective. Overwriting consists of recording data onto magnetic media by writing a pattern of binary ones (1) and zeros (0). These patterns can then be read back and interpreted as individual bits, eight (8) of which are used to represent a byte or character. If the data is properly overwritten with a pattern (e.g., “11111111” followed by “00000000”) the magnetic fluxes will be physically changed and the drive’s read/write heads will only detect the new pattern and the previous data will be effectively erased. To purge a hard drive requires overwriting with a pattern and then its complement, and finally with another pattern (e.g., overwrite first with “00110101,” followed by “11001010” then “10010111”). Sanitization is not complete until all six passes of the three cycles are completed.

b. Data-overwriting Software.

Another method for sanitizing storage media is using commercial software. Certain software can be used but it must meet the criteria listed below, Paragraph 7, Acceptable Commercial Software Products, of this appendix. Software products and applications not meeting the stated minimum specifications are not acceptable for sanitizing SBU storage media. Overwriting software that reformats or repartitions a hard drive will not be accepted within the scope of this policy. Also, some software product versions may not have the capability to remove the OS during the overwrite process. To ensure the integrity of the sanitization process, overwriting software must have the following functions and capabilities:

(1) The ability to purge all data or information, including the Operating System (OS), from the physical or virtual drives, thereby making it impossible to recover any meaningful data by keyboard or laboratory attack,

(2) A compatibility with, or capability to run independent of, the OS loaded on the hard drive,

(3) A compatibility with, or capability to run independent of, the type of hard drive being sanitized (e.g., Advanced Technology Attachment (ATA)/Integrated Drive Electronics (IDE) or Small Computer System Interface (SCSI) type hard drives),

(4) A capability to overwrite the entire hard disk drive independent of any Basic Input/Output System (BIOS) or firmware capacity limitation that the system may have,

(5) A capability to overwrite using a minimum of three cycles (six passes) of data patterns on all sectors, blocks, tracks, and slack or unused disk space on the entire hard disk medium,

(6) A method to verify that all data has been removed from the entire hard drive and to review the overwrite pattern.

c. Degaussing.

Degaussing is a procedure that reduces the magnetic flux of a medium to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously-stored data on magnetic media unreadable. The drawback to degaussing is that very seldom can a drive be used after this process. For a degausser to be effective here are a few standards and procedures which must be used:

(1) Degaussers used on FAA hard drives must have a nominal rating of at least 1700 Oersted.

(2) Degaussers must be operated at their full magnetic strength.

(3) The product manufacturer's directions must be carefully followed. Deviations from an approved method or rate of coercivity could leave significant portions of data remaining on a hard drive.

(4) All shielding materials (e.g., castings, cabinets, and mounting brackets) which may interfere with the degausser's magnetic field must be removed from the hard drive before degaussing.

(5) Hard disk platters must be in a horizontal direction during the degaussing process.

(6) For degaussing hard drives with very high coercivity ratings, it may be necessary to remove the magnetic platters from the hard drive's housing.

(7) Degaussing products should be acquired from the National Security Agency's (NSA) Degausser Products List which can be obtained by contacting:

National Security Agency
Attn: S7 Media Technology Center
9800 Savage Road, Ft. George G. Meade, MD 20755-6877
Tel: 1 (800) 688-6115 (Option #3) or 1 (410) 854-7661
Fax: 1 (410) 854-7668.

d. Destruction of Media.

Destruction of media is generally used when a disk has damaged or unusable tracks and sectors and the disk is not reusable. Authority to destroy the media must be obtained from the Property Custodian before proceeding. Destruction of storage media is the process of physically damaging a medium so that it is not usable in a computer, and so that no known exploitation method can retrieve data from it. If possible, operable media should be overwritten or degaussed prior to destruction. The three acceptable methods of destruction are:

(1) Physical destruction/impairment beyond reasonable use: Remove the hard drive from the chassis or cabinet. Remove any steel shielding materials, mounting brackets, and cut any electrical connection to the hard drive unit. In a suitable facility with individuals wearing appropriate safety equipment, subject the hard drive to physical force (i.e., pounding with a sledgehammer) that will disfigure, bend, mangle, or otherwise mutilate the hard drive so that it cannot be re-inserted into a functioning computer. Sufficient force should be used directly on top of the hard drive unit to cause shock/damage to the disk surfaces. In addition, any connectors that interface into the computer must be mangled, bent, or otherwise damaged to the point that the hard drive could not be re-connected without significant rework.

(2) Destruction at a metal destruction facility, (i.e., smelting, disintegration, or pulverization).

(3) Application of an abrasive substance (emery wheel or disk sander) to a magnetic disk or drum recording surface. Make certain that the entire recording surface is completely removed. Ensure proper safety measures, to include protection from inhaling abraded dust and use of protective eyewear.

A3-6. Definitions.

a. Clearing — Rendering stored information unrecoverable unless special utility software or techniques are used.

b. Degaussing — Reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used as a method of sanitization.

c. Media — Short for storage media. Physical objects on which data can be stored, such as hard drives, floppy disks, Compact Disks (CD)-Read-Only Memory (ROM) (CD-ROM), and tapes.

d. Overwriting — Process of writing patterns of data on top of the data stored on a magnetic medium.

e. Oerstad — A unit of magnetic field strength.

f. Sanitize — To expunge data from storage media so that data recovery is impossible. Sanitizing includes overwriting, degaussing, and destruction (destruction is not an appropriate means for TOS purposes). Clearing data does not constitute sanitizing.

g. SBU Information — SBU information is any information the loss, misuse, or unauthorized access to, or modification of, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (The Privacy Act), but which has not been specifically authorized under criteria established by Executive Order or an Act of Congress, to be kept secret in the interest of national defense or foreign policy. This includes information in routine FAA payroll, finance, logistics, and personnel management systems.

A3-7. Acceptable Commercial Software Products. The following commercial software is of acceptable use for overwriting computer storage media. This is not to be considered an all-inclusive list, as there are other products that meet the minimum requirements, but this list

should be used as a reference. This list is subject to change and should only be used as a reference.

- a. Product Name: “No Trace”
Communication Technologies, Inc.,
14151 Newbrook Dr., Suite 400, Herndon, VA 20170
Tel: (703) 961-9080
www.comtechnologies.com
- b. Product Name: “DataEraser”
ONTRACK Data International, Inc.
Tel: 1 (800) 872-2599
www.ontrack.com
- c. Product Name: “UniShred Pro”
Los Altos Technologies
Tel: (919) 233-9889
www.lat.com
- d. Product Name: “CleanDrive”
Access Data Corporation
(800) 574-5199
www.accessdata.com
- e. Product Name: “Sanitizer D 4.01”
Infraworks
(512) 583-5000
www.infraworks.com/products/sanitizer.html

This page intentionally left blank.

Appendix 4. Administrative Information

A4-1. Distribution. This directive is distributed to selected offices and facilities with the following Facility, Service, and Equipment Profile (FSEP) equipment: Time Based Flow Management (TBFM).

a. To subscribe to email notifications of issued Maintenance Technical Handbooks (MTHB):

(1) Go to <http://dis.faa.gov>. Click Subscribe. Click Subscribe to List. Enter your email address. Click Display Subscription Options. Select the series of MTHB for subscription. Click Subscribe.

or

(2) Go to https://employees.faa.gov/tools_resources/orders_notices. Select the series of MTHB for subscription. Click Go. Enter your email address. Click Go. Confirm email address, click radio button under Optional Password. Enter password if password was selected. Click Save.

b. For an electronic copy of this MTHB, go to:
https://employees.faa.gov/tools_resources/orders_notices/.

A4-2. Authority to Change this Order. En Route & Oceanic Services Second Level Engineering (SLE), TBFM, is the Office of Primary Responsibility (OPR) for this directive, and has the authority to change and update this directive as needed. This handbook is under configuration management control as defined in Order 1800.66, Configuration Management Policy, and NAS-MD-001, National Airspace System Master Configuration Index Subsystem Baseline Configuration and Documentation Listing. Any changes to the baseline document or requests for deviation from national standards shall be processed through the NAS Change Proposal (NCP) process. Copies of FAA form 1800-2, NAS Change Proposal, are provided in the back of this handbook for the convenience of handbook users.

A4-3. Related Publications.

Order 1000.37	Air Traffic Organization Safety Management System
Order 1100.161	Air Traffic Safety Oversight
Order 1370.81	Electronic Mail Policy
Order 1370.82	Information Systems Security Program
Order 1600.2	Safeguarding Controls and Procedures for Classified National Security Information and Sensitive Unclassified Information
Order 1600.75	Protecting Sensitive Unclassified Information (SUI)
Order 1800.66	Configuration Management Policy
Order 6000.15	General Maintenance Handbook for National Airspace System (NAS) Facilities

Order JO 6000.50	National Airspace System (NAS) Integrated Risk Management
Order 6032.1	National Airspace System (NAS) Modification Program
Order 8020.11	Aircraft Accident and Incident Notification, Investigation, and Reporting
Order 8020.16	Air Traffic Organization Aircraft Accident and Incident Notification, Investigation, and Reporting
NAS-MD-001	National Airspace System Master Configuration Index Subsystem Baseline Configuration and Documentation Listing
FAA-G-2100	Electronic Equipment General Requirement
TI 6480.8	System Administration Manual, Time Based Flow Management

A4-4. Forms and Reports. Any forms or reports referenced in this document may be found at https://employees.faa.gov/tools_resources/forms/index.cfm.

A4-5. Recommendations for Changes. Forward any requests or recommendations for changes to the TBFM SLE team via the En Route & Oceanic Support Help Desk at 1-800-377-0308, or access the website at <https://enroutesupport.faa.gov>.

Appendix 5. Safety Risk Management Decision Memorandum

DRAFT

This page intentionally left blank.

CASE FILE/ NAS CHANGE

(PLEASE TYPE OR PRINT NEATLY)

Page 1 of _____

1. Case File Number		2. For CM Use		Case File Received Date	NCP Issuance Date	NCP Number
3. Scope of Change <input type="checkbox"/> Local <input type="checkbox"/> National <input type="checkbox"/> Test		4. Reason For Change <input type="checkbox"/> Safety <input type="checkbox"/> Technical Upgrade <input type="checkbox"/> Systems Interface <input type="checkbox"/> Requirements Change <input type="checkbox"/> Design Error <input type="checkbox"/> Parts Unavailability <input type="checkbox"/> Baseline <input type="checkbox"/> Other				
5. Priority <input type="checkbox"/> Normal <input type="checkbox"/> Time-Critical <input type="checkbox"/> Urgent	6. Justification of Time Critical/Urgent Priority			7. Supplemental Change Form <input type="checkbox"/> ECR/ECP <input type="checkbox"/> TES <input type="checkbox"/> N/A 7a. Supplemental Change No. _____ 7b. Supplemental Change Initiation Date _____		
8. Case File Originator		9. Originator's Organization		10. Telephone Number		11. Case File Initiation Date
12. Type of Document Affected <input type="checkbox"/> CPFS <input type="checkbox"/> SPEC <input type="checkbox"/> MTBK <input type="checkbox"/> _____ <input type="checkbox"/> TI <input type="checkbox"/> DWG <input type="checkbox"/> IRD/ICD				13. Baseline Document Number(s)		
14. CI Subsystem Designator		15. FA _		16. CI Component Designator		
17. Facility Identifier (FACID)		18. Facility Code (FACCODE)		19. Cost Center Code		20. Software System Version
21.						
22. Description: (a) identification of problem, (b) proposed change, (c) interface impact, (d) cost estimate (e) funding source (f) benefits/risks, (g) Schedule (h) Other (e.g. logistics, quality, etc.) (a) (b) (c) (d) (e) (f) (g) (h)						

Blocks 1 through 22 are to be completed by originator and/or the NCP coordinator. If a block is not applicable, write n/a. Attach additional sheets if necessary. See current revision of NAS-MD-001 for detailed completion instructions.

Case File Number					NCP Number					Page 2 of ____	
23. Name and Title of Originator's Immediate Supervisor (Type/Print Clearly)					Signature					Date	
24. Facility/SMO Review (AT/AF)					25. Regional Review						
Name	Routing Symbol	Date	Concur	Non-Concur	Name	Routing Symbol	Date	Concur	Non-Concur		
					<input type="checkbox"/> Recommend Approval <input type="checkbox"/> Disapprove <small>(Enter into CM/STAT. Forward to Prescreening) (Return to Originator)</small>						
Routing Symbol	Signature				Routing Symbol	Signature					
Date					Date						
Routing Symbol	Signature				Routing Symbol	Signature					
Date					Date						
24a. Comments					Routing Symbol	Signature/Configuration Mgr/NCP Coordinator/ Reg Exec Sec					
					Date						
25a. Comments											
(Attach additional sheets if necessary)					(Attach additional sheets if necessary)						
<div style="display: flex; justify-content: space-between;"> 26. PRESCREENING </div>											
Prescreening Office _____ Prescreening Comments:											
(Attach additional sheets if necessary)											
Reviewers	Routing Symbol	Date	Concur	Non-Concur	<input type="checkbox"/> Recommend Approval <input type="checkbox"/> Recommend Disapproval <input type="checkbox"/> New Requirement <small>(Return original to originating office through the Regional NCP Coordinator)</small>						
Recommended Must Evaluators					Routing Symbol	Signature					
					Date						
27. For Internal Configuration Management Use Only											